AMENDMENTS TO THE CLAIMS

According to the Notice of Allowance mailed on October 31, 2008, claims 1-2, 4-12 and 24-48 are allowed in the instant application. However, the Notice of Allowance erroneously states that Claim 37 was allowed. Claim 37 was previously cancelled in a Response Under 37 C.F.R. § 1.133, which was electronically filed on September 22, 2008. Claims 1, 11, 21 and 35 have been amended to clarify the claims and to further correct an antecedent basis issue. The Applicant submits that no claim limitations were removed and that no new matter has been added to any of claims 1, 11, 21 and 35.

The Applicant requests reconsideration of the claims in view of the following amendments reflected in the listing of claims.

Listing of claims:

1. (Currently amended) A method for producing a secure key, the method comprising:

receiving a plurality of input keys comprising a first input key, a second input key and a third input key;

generating a first output key based on said plurality of input keys comprising said first input key, said second input key and said third input key[[,]]; and

continuing said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys, wherein said first output key is unique and differs from said at least one of said plurality of input keys, and said at least one of said plurality of input keys is a key variation comprising a device identity~~; and~~

~~continuing said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys~~.

2. (Previously presented) The method according to claim 1, wherein said first input key is a customer key, and/or a customer key selection.

3. (Cancelled)

4. (Previously presented) The method according to claim 1, comprising determining whether said first output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

5. (Previously presented) The method according to claim 4, wherein said first output key is not a weak or semi-weak key.

6. (Previously presented) The method according to claim 1, comprising mapping said at least said first input key, said second input key and said third input key to generate mapped output key data.

7. (Previously presented) The method according to claim 6, comprising generating an intermediate key based on said first input key.

8. (Previously presented) The method according to claim 7, comprising scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output.

9. (Previously presented) The method according to claim 8, comprising:

masking at least a portion of said generated mapped output key data; and

exclusive ORing said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

10. (Previously presented) The method according to claim 1, comprising transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

11. (Currently amended) A machine-readable storage having stored thereon, a computer program having at least one code section for producing a secure key, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

receiving a plurality of input keys comprising a first input key, a second input key and a third input key;

generating a first output key based on said plurality of input keys comprising said first input key, said second input key and said third input key[[,]]; and

continuing said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys, wherein said first output key is unique and differs from said at least one of said plurality of input keys, and said at least one of said plurality of input keys is a key variation comprising a device identity~~; and~~

~~continuing said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys~~.

12. (Previously presented) The machine-readable storage according to claim 11, wherein said first input key is a customer key, and/or a customer key selection.

13. (Cancelled)

14. (Previously presented) The machine-readable storage according to claim 11, wherein said at least one code section comprises code for determining whether said first output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

15. (Previously presented) The machine-readable storage according to claim 14, wherein said first output key is not a weak or semi-weak key.

16. (Previously presented) The machine-readable storage according to claim 11, wherein said at least one code section comprises code for mapping said at least said first input key, said second input key and said third input key to generate mapped output key data.

17. (Previously presented) The machine-readable storage according to claim 16, wherein said at least one code section comprises code for generating an intermediate key based on said first input key.

18. (Previously presented) The machine-readable storage according to claim 17, wherein said at least one code section comprises code for scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output.

19. (Previously presented) The machine-readable storage according to claim 18, wherein said at least one code section comprises:

code for masking at least a portion of said generated mapped output key data; and

code for exclusive ORing said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

20. (Previously presented) The machine-readable storage according to claim 11, wherein said at least one code section comprises code for transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

21. (Currently amended) A system for producing a secure key, the system comprising:

a secure key generator that receives a plurality of input keys comprising a first input key, a second input key and a third input key;

said secure key generator generates a first output key based on said plurality of input keys comprising said first input key, said second input key and said third input key~~,~~; and

said secure key generator continues said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys, wherein said first output key is unique and differs from said at least one of said plurality of input keys, and said at least one of said plurality of input keys is a key variation comprising a device identity~~; and~~

~~said secure key generator continues said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys~~.

22. (Previously presented) The system according to claim 21, wherein said first input key is a customer key, and/or a customer key selection.

23. (Cancelled)

24. (Previously presented) The system according to claim 21, wherein said secure key generator determines whether said first output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

25. (Previously presented) The system according to claim 24, wherein said first output key is not a weak or semi-weak key.

26. (Previously presented) The system according to claim 21, comprising a mapper that maps said at least said first input key, said second input key and said third input key to generate mapped output key data.

27. (Previously presented) The system according to claim 26, comprising a key generator that generates an intermediate key based on said first input key.

28. (Previously presented) The system according to claim 27, comprising a scrambler that scrambles said generated intermediate key and said generated mapped output key data to create a scrambled output.

29. (Previously presented) The system according to claim 28, comprising:

a masker that masks at least a portion of said generated mapped output key data; and

an exclusive OR operator that exclusive ORs said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

30. (Original) The system according to claim 21, wherein said secure key generator transfers said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

31. (Original) A system for producing a secure key, the system comprising:

a mapper;

a scrambler coupled to said mapper;

a masker coupled to said mapper;

a key generator coupled to said scrambler; and

an XOR operator coupled to said masker and said scrambler.

32. (Previously presented) The system according to claim 31, comprising at least one processor coupled to an output of said XOR operator.

33. (Previously presented) The system according to claim 32, comprising an encryption engine that is coupled to an output of said XOR operator.

34. (Previously presented) The system according to claim 33, comprising a memory coupled to at least one of said encryption engine and said at least one processor.

35. (Currently amended) A system for producing a secure key, the system comprising:

one or more circuits enabled to:

receive a plurality of input keys comprising a first input key, a second input key and a third input key at a secure key generator;

generate at said secure key generator a first output key based on said plurality of input keys comprising said first input key, said second input key and said third input key [[,]]; and

continue said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys, wherein said first output key is unique and differs from said at least one of said plurality of input keys, and ~~wherein~~ said at least one of said plurality of input keys is a key variation comprising a device identity~~; and~~

~~continue said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys~~.

36. (Previously presented) The system according to claim 35, wherein said first input key is a customer key, and/or a customer key.

37. (Cancelled)

38. (Previously presented) The system according to claim 35, wherein said one or more circuits determine whether said first output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

39. (Previously presented) The system according to claim 38, wherein said first output key is not a weak or semi-weak key.

40. (Previously presented) The system according to claim 35, wherein said one or more circuits comprise a mapper that maps said at least said first input

key, said second input key and said third input key to generate mapped output key data.

41. (Previously presented) The system according to claim 40, wherein said one or more circuits comprise a key generator that generates an intermediate key based on said first input key.

42. (Previously presented) The system according to claim 41, wherein said one or more circuits comprise a scrambler that scrambles said generated intermediate key and said generated mapped output key data to create a scrambled output.

43. (Previously presented) The system according to claim 42, wherein said one or more circuits comprise:

a masker that masks at least a portion of said generated mapped output key data; and

an exclusive OR operator that exclusive ORs said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

44. (Previously presented) The system according to claim 35, wherein said one or more circuits transfer said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

45. (Previously presented) A system for producing a secure key, the system comprising one or more circuits, said one or more circuits enabled to operate as:

a mapper;

a scrambler coupled to said mapper;

a masker coupled to said mapper;

a key generator coupled to said scrambler; and

an XOR operator coupled to said masker and said scrambler.

46. (Previously presented) The system according to claim 45, wherein said one or more circuits comprise at least one processor coupled to an output of said XOR operator.

47. (Previously presented) The system according to claim 46, wherein said one or more circuits comprise an encryption engine that is coupled to an output of said XOR operator.

48. (Previously presented) The system according to claim 47, wherein said one or more circuits comprise a memory coupled to at least one of said encryption engine and said at least one processor.